Journal of Theoretical and Applied Information Technology
15th June 2017. Vol.95. No 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DYNAMIC MULTICAST TREE MAINTENANCE PROTOCOL FOR SECURE GROUP COMMUNICATION IN MANET

[1]G.NARAYANA, [2] M.AKKALAKSHMI , [3]A.DAMODARAM

[1]Associate Professor,Dept of CSE,Joginpally B.R Engg.College,Hyderabad,Telangana, India
[2]Professor, Dept of IT, GITAMS Uiversity,Hyderabad, Telangana,India
[3]Vice-Chancellor, Sri Venkateswara University, Tirupati, Andhrapradesh, India
Email: narayangphd@gmail.com

ABSTRACT

In mobile ad hoc network (MANET), the nodes communicate wirelessly through multiple hops as it has several nodes inside each network. Each node can enter and leave the network in a dynamic way without having any restriction in its mobility. Group key management technique is employed for ensuring security and integrity in MANET. When devised appropriately, this technique offers security to the data in the network with high key computation cost and overhead. This is because there is a need to compute the group key every time a new node joins or leaves the network. To overcome this issue, we have proposed a dynamic multicast tree maintenance protocol for secure group communications. When a new node enters the network or leaves the network, only the subtree involved with the node joining or node departure needs to recompute a group key. The group key of remaining part of the multicast tree will not be changed. Simulation results show that this process reduces overhead and unnecessary key computation process, thereby enhancing the network performance.
Keywords: *MANET, Multicast Tree, Group Communication, Protocol, AODV, DSR*

1. INTRODUCTION

1.1 Mobile Adhoc Network (MANET)

MANET consists of a numerous independent nodes, also called as users, linked to one another wirelessly through multiple hops. Every node can act as a sender for transmitting data, as a receiver for collecting the data for subsequent operation, and as a router for routing the data along the wireless medium when the communication is between different transmission range. Node can move individually in a dynamic manner. Since there is no central access point or central administrator, it does not face any restriction [1]. As the current world uses wireless medium for most of the applications, MANETs are employed in several applications such as military operations like battlefield communication which can be communication between two warship, or soldiers, commercial purposes like online events, online meetings. Some of the issues faced by MANET are security issues due to attacks from hackers and malicious nodes, resource limitations, channel degradation, and so forth [2].

1.2 Significance and Scope

It is necessary to perform communication in a secure manner when sensitive data is being transmitted.

Group key management (GKM) is the fundamental component of secure group communication systems that involves distribution, updation and revocation of group keys. GKM can be carried out using centralized and distributed group key distribution approaches [3].

In GKM, a common secret key which is referred as a group key, is essential for ensuring the integrity and confidentiality of group messages that is being transmitted [4] [5].

Some of the factors restricting secure group management in MANET are: node mobility, scalability, limited computing power, multi-hop wireless channel and lack of infrastructure [1]

1.3 Motivation and Objectives

In our previous works [10][11], an Energy-Efficient Polynomial-Based Group Key

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Management Protocol for Secure Group Communications is proposed based on polynomial group key handling method. In this protocol, a group manager (GM) who is initially chosen based on link quality and residual energy is responsible for creating polynomials for both intra- and intergroup communication. New group manager is chosen when the residual energy or the link quality of the group manager reduces beyond a particular level, indicating that this technique works in a self-organizing manner.

Secure key generation and re-keying without increasing the storage and communication overhead, is really challenging in MANET.

The system performs group key reconstructions frequently whenever mobile nodes dynamically join or leave the networks. However, the cost of communication and key management during dynamic join and leave of group members is more.

Hence the main objective of this work is to reduce the cost and the overhead of security management for improving the quality of service (QoS) in MANET.

In order to meet this objective, this paper proposes a dynamic multicast tree maintenance protocol for secure group communications in MANET.

2. RELATED WORKS

V. Palanisamy et al [6] have proposed a Secure Group Communication using Multicast Key Distribution Scheme in Ad hoc Network where multicast key distribution technique is used that includes a key tree-based group key distribution. Here, data encryption is performed with the help of group key for ensuring confidentiality. Group rekeying process is initiated whenever there is any variation in the group members for enhancing the overall security. But the group selection process discussed in this paper did not consider the energy efficiency and link quality metrics. Moreover, the cost of keying and re-keying will be high.

B. Gopalakrishnan et al [7] have proposed Energy-Efficient Transitive Signature Scheme for Secure Group Communication in MANETs in which groups are formed using an energy-efficient routing scheme. While communication occurs between different group members, a transitive signature scheme is used to improve the security. When any variation in the node membership is observed, each node can enter and exit a group in a random manner through rekeying function. But frequent change in topology and routing, causes high rekeying cost.

N. Vimala et al [8] have proposed Efficient Group Key Management Protocol for Region Based MANETs where a member node is considered as a group coordinator for calculating and distributing the keying details to the intermediate nodes within the group. Each member of the node determines the group key in a distributed fashion. Every group member is given the responsibility of functioning as a group coordinator in an alternating manner for dividing the work of group rekeying and group maintenance. A new key tree structure is presented to smoothly handover the group coordinator functionality from one member node to another. But the cost involved in keying and rekeying will be huge.

Hua-Yi Lin et al [9] have proposed Efficient Key Agreements in Dynamic Multicast Height Balanced Tree for Secure Multicast Communications in Ad Hoc Networks that provide high security as provided by the RSA and Diffe-Hellman algorithm. It allows nodes to enter and exit the network dynamically. To ensure security during multicasting of data, ECDH key function is used along with the hash operation. As a result of this, they avoided the complicated network operations. Simulation results show that this mechanism is better when compared with the conventional techniques in terms of networking expenses, performance, overhead, and so forth. Though this work provide technique for reducing the keying cost, it lacks a self-organized group establishment procedure.

From the above discussion, it can be observed that the existing works on GKM do not guarantee the QoS during group head selection and reducing the cost and overhead. Hence the proposed DMTM protocol mainly handles these issues.

3. DYNAMIC MULTICAST TREE MAINTENANCE (DMTM) PROTOCOL

3.1 Overview

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In this work, Dynamic Multicast tree maintenance protocol, the joining or leaving node in a group is identified and only the key value from the part of the joining (leaving) node subtree is recomputed without recomputing the entire tree, thus saving a tremendous amount of operational time. For joining and leaving, the Dynamic Multicast Height Balanced Group Key Agreement (DMHBGKA) Insert and Remove algorithms [9] are used in which the group key is constructed as per our second work.

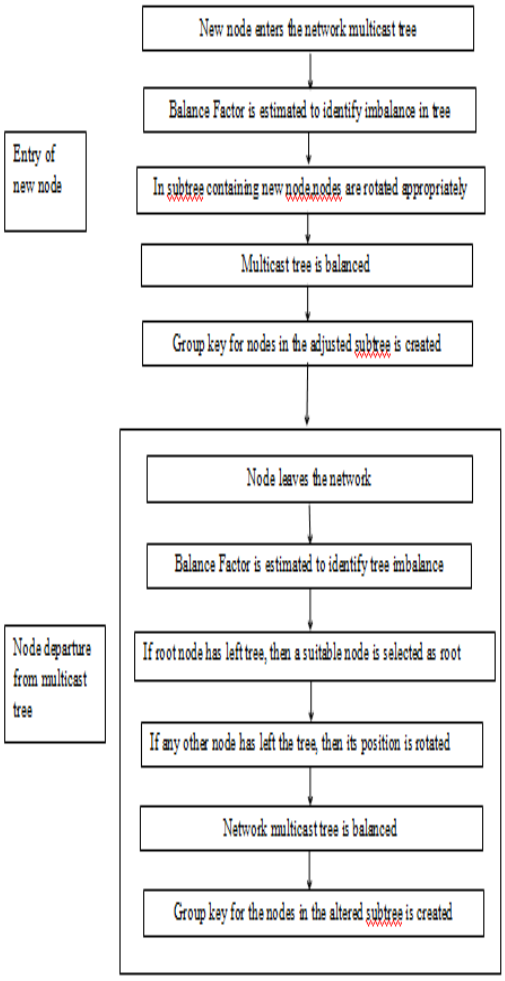

Figure.1: Block Diagram

3.2 DMHBGKA for joining nodes

In the multicast tree, every node from the root node to the leaf node has a group key as seen in the previous paper. But when a new node joins the multicast tree, the node has to be placed such as to adjust the tree balance. Then the group id for the new node has to be determined. This process is described in algorithm 1.

Algorithm 1

Notations:

1. BF : Balance Factor
2. N_L : Number of nodes in left tree
3. N_R : Number of nodes in right tree
4. $G_{x(i)}$: private key of the group member
5. k : random secret selected by parent node
6. KEK_i : Key Encryption Key of a group member
7. i : integer number
8. X_i : locked encryption key
9. G_k mod p: parent node signature key
10. p : predefined large prime number
11. P : Polynomial
12. x : variable where the respective KEK has to be deployed

Algorithm:

1. When a new node joins the multicast tree, the node is initially placed in the tree depending on its IP/MAC address as shown in figure 2.

2. BF is estimated using equation (1).

$$BF = N_L - N_R \quad (1)$$

3. If BF = 0, 1, or -1, the tree will be considered to be balanced.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. If |BF| > 1, tree will be considered to be unbalanced.

4.a. If BF > 1 (the left tree is greater than right tree), the child node in the left most subtree will be rotated once.

4.b. If BF < -1 (the right tree is greater than left tree), the child node in the right most subtree will be rotated once (as shown in figure 3).

5. Once the tree is balanced after adjusting the newly joined node/nodes position, it requires a group id from its parent node.

6.This newly joined node sends an GRP_REQ message after signing it with its private key, $G_{x(i)}$ to its parent node.

9. The parent node selects a random secret, k and computes KEK_i and signs it with its private lock secret key and locks it according to equation (3).

$$(X_i)_k = (G_{x(i)})_k \quad (3)$$

10. Then the parent node sends the locked KEK_i to the newly joined node.

11. On receiving the locked KEK_i, the newly joined node verifies the parent node signature by unlocking it with its private unlock secret key according to equation (4).

$$KEK_i = ((X_i)_k)_{y(i)} \bmod p = (G_{x(i).y(i)})_k \bmod p = G_k \bmod p \quad (4)$$

12. If the newly joined node determines the parent signature to be invalid then it ignores the received broadcast message, else it accepts it.

13. Then parent node generates a polynomial P using the KEK_i as shown in equation (5) and sent to the newly joined node after locking it by lock secret for security purpose.

$$P = (x - KEK_1) + (x - KEK_2) + .. + (x - KEK_n) + G_k \quad (5)$$

14. On receiving the P, the newly joined node computes the group key by using its own KEK_i.

$$\text{group key} = (x - KEK_i) + G_k \quad \text{with } x = KEK_i \quad (4)$$

$$\text{group key} = 0 + G_k$$

$$\text{group key} = G_k$$

15. Using the unlock secret, the newly joined node extracts the P received from parent node.

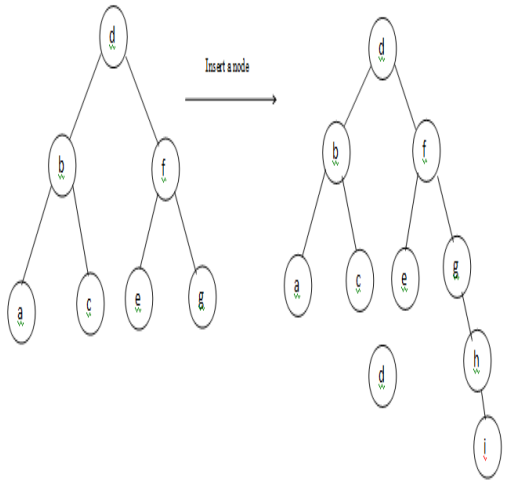

Figure.2: Multicast Tree with newly joined nodes

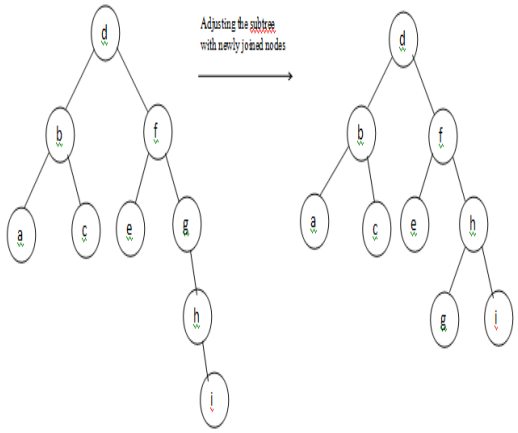

Figure.3: Node location adjustment of the subtree with newly joined nodes

In this way, as the new nodes join the network tree, the node position is adjusted to balance the multicast tree to overcome imbalance in the tree structure.

3.3 DMHBGKA for leaving nodes

When a node leaves the multicast tree, its position becomes vacant and it may sometimes

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

lead to imbalance in the multicast tree structure. So, after any node leaves the tree, the tree needs to adjusted to maintain balance if required. Then the group id of the nodes whose position is altered in the tree has to be determined. This process is described in algorithm 2.

Algorithm 2

Notations:

4. BF : Balance Factor

5. N_L : Number of nodes in left tree

6. N_R : Number of nodes in right tree

4. $G_{x(i)}$: private key of the group member

5. k : random secret selected by parent node

6. KEK_i : Key Encryption Key of a group member

7. i : integer number

8. X_i : locked encryption key

9. G_k mod p: parent node signature key

10. p : predefined large prime number

11. P : Polynomial

12. x : variable where the respective KEK has to be deployed

Algorithm:

1. When a node leaves the multicast tree, the node position is initially left empty (as shown in figure 5).

2. BF is estimated using equation (6).

$$BF = N_L - N_R \quad (6)$$

3. If BF = 0, 1, or -1, the tree will be considered to be balanced; otherwise, it will be imbalanced.

4. If |BF| > 1 and the node which has left is the root node (as shown in figure 4)

4.a. If BF > 1 (the left tree is greater than right tree), then the largest node in the left subtree will be selected as root node.

4.b. If BF < -1 (the right tree is greater than left tree), then the smallest node in the right subtree will be selected as root node.

5. If |BF| > 1 and the node which has left is not a root node,

5.a. If BF > 1 (the left tree is greater than right tree), then the largest node in the leftmost subtree will be rotated once.

5.b. If BF < -1 (the right tree is greater than left tree), then the smallest node in the right subtree will be rotated (as shown in figure 6).

6. Once the tree is balanced after adjusting the position of the existing nodes, then all the nodes with altered position requires a group id from its parent node.

7.The nodes with altered position sends an GRP_REQ message after signing it with its private key, $G_{x(i)}$ to its parent node.

8. The parent node selects a random secret, k and computes KEK_i and signs it with its private lock secret key and locks it according to equation (3).

$$(X_i)_k = (G_{x(i)})_k \quad (3)$$

9. Then the parent node sends the locked KEK_i to the requesting node.

10. On receiving the locked KEK_i, the requesting node verifies the parent node signature by unlocking it with its private unlock secret key according to equation (4).

$$KEK_i = ((X_i)_k)_{y(i)} \bmod p = (G_{x(i).y(i)})_k \bmod p = G_k \bmod p \quad (4)$$

11. If the requesting node determines the parent signature to be invalid then it ignores the received broadcast message, else it accepts it.

12. Then parent node generates a polynomial P using the KEK_i as shown in equation (5) and sent to the requesting node after locking it by lock secret for security purpose.

$$P = (x - KEK_1) + (x - KEK_2) + .. + (x - KEK_n) + G_k \quad (5)$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

13. On receiving the P, the requesting node computes the group key by using its own KEK_i.

$$\text{group key} = (x - KEK_1) + (x - KEK_2) + .. + (x - KEK_n) + G_k \quad \text{with } x = KEK_i \quad (4)$$

$$\text{group key} = 0 + G_k$$

$$\text{group key} = G_k$$

14. Using the unlock secret, the newly joined node extracts the P received from parent node.

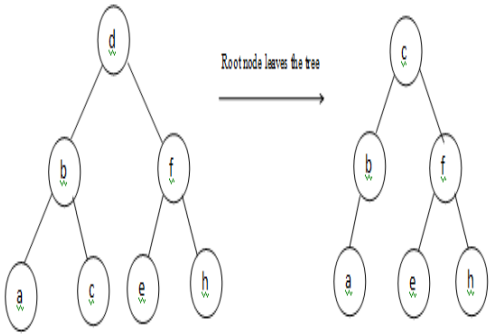

Figure.4: Root node leaving the tree

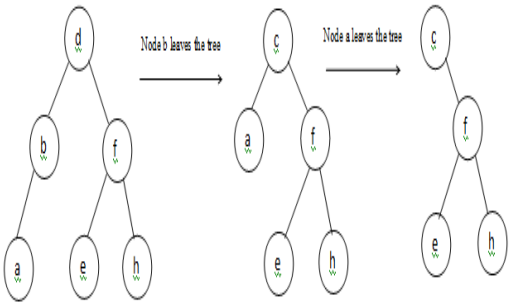

Figure.5: Non root node leaving the tree

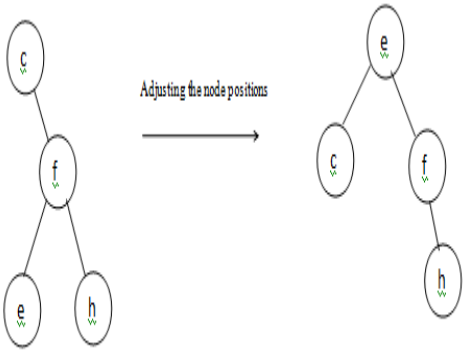

Figure.6: Balancing the tree after member nodes leave

Thus, as every node depart from the multicast tree, the position of the remaining nodes are adjusted to avoid imbalance in the multicast tree.

4. SIMULATION RESULTS

Network simulator-2 (NS2) is used to simulate our proposed Dynamic Multicast Tree Maintenance Protocol (DMTM) protocol. The area size is 1000 x 1000 m^2 region for simulation time of 50 s. The simulated traffic is Constant Bit Rate (CBR).

The security provided by the GKM technique is measured using the packet drop and packet delivery ratio metrics. The efficiency of the GKM technique is measured using the average residual energy, authentication delay and overhead metrics. The Packet Delivery Ratio (PDR) is the ratio of the number of packets received successfully and the total number of packets transmitted. Residual Energy is the amount of energy remains in the nodes after the data transmission.

The simulation settings and parameters are summarized in table 1.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: Simulation parameters

No. of Nodes	50
Area	1000 X 1000
MAC	802.11
Simulation Time	50 sec
Traffic Source	CBR
Attackers	2,4,6,8 and 10
Propagation	TwoRayGround
Antenna	OmniAntenna
Initial Energy	10.1J
Transmission Power	0.3
Receiving Power	0.3

4.1 Performance Metrics

The proposed DMTM protocol is compared with the dynamic multicast height balanced group key agreement (DMHBGKA) [9] protocol.

4.2 Results & Analysis

The simulation results are presented in this section.

A. Based on Attackers

In order to evaluate the impact of node compromise attacks, the number of attackers is varied as 2, 4, 6, 8, and 10.

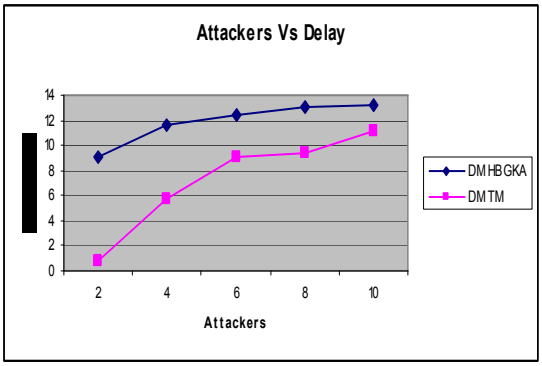

Figure 7: Attackers Vs Delay

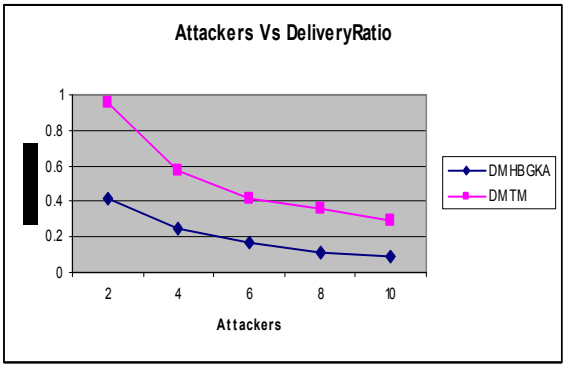

Figure 8: Attackers Vs Delivery Ratio

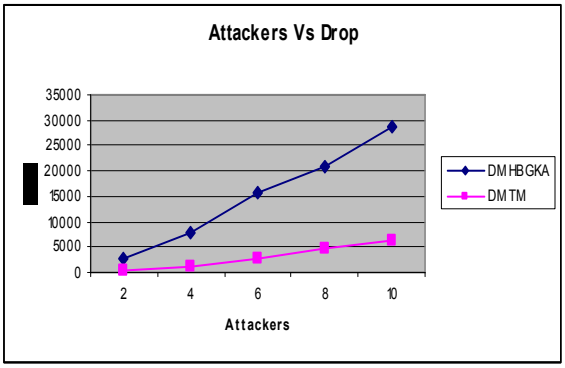

Figure 9: Attackers Vs Drop

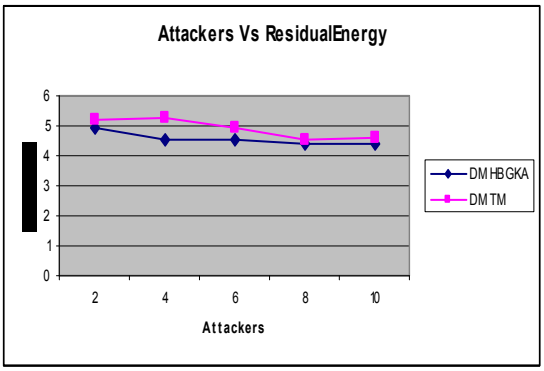

Figure 10: Attackers Vs Residual Energy

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

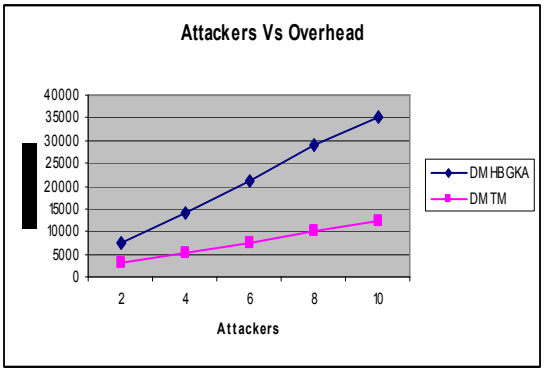

Figure 11: Attackers Vs Overhead

Figure 7 shows the authentication delay measured for DMHBGKA and DMTM when the number of attackers is varied. When the number of attackers is increased from 2 to 10 the delay of DMHBGKA and DMTM increase, as seen from the figure. However, the average delay of DMTM is 42% less when compared to DMHBGKA, since it involves polynomial based group key generation process, which is less complex when compared to ECDH of DMHBGKA.

Figure 8 shows the packet delivery ratio measured for DMHBGKA and DMTM when the number of attackers is varied. When the attackers are increased from 2 to 10 the delivery ratio of DMHBGKA and DMTM decreases, as seen from the figure. Since DMTM provides both intra and inter GKM, the average packet delivery ratio of DMTM is 62% higher than DMHBGKA.

Figure 9 shows the packet drop measured for DMHBGKA and DMTM when the number of attackers is varied. When the number of attackers is increased, the packet drop both the techniques is increased. Since DMTM provides both intra and inter GKM, the average packet drop of DMTM is 82% low when compared to DMHBGKA.

Figure 10 shows the average residual energy measured for DMHBGKA and DMTM when the number of attackers is varied. When the attackers is increased, the residual energy of both the techniques decreases. Since DMTM selects the group heads based on their energy level, the average residual energy of DMTM is 7% lesser than DMHBGKA.

Figure 11 shows the overhead measured for DMHBGKA and DMTM when the number of attackers is varied. When the attackers are increased from 2 to 10, the overhead of DMHBGKA and DMTM is increased. But DMTM has 64% lesser overhead when compared to DMHBGKA.

B. Based on PauseTime

In order to evaluate effect of mobility and frequent topology changing, the pause time of the nodes is varied as 5,10,15,20 and 25sec.

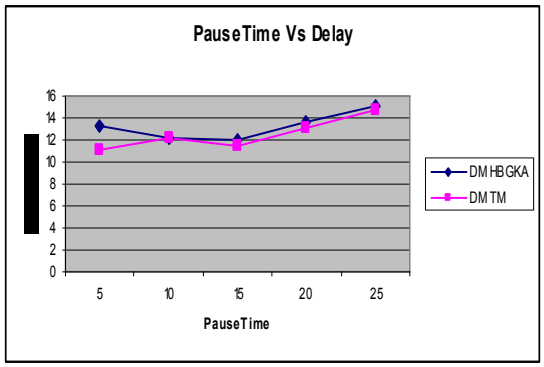

Figure 12: Pause Time Vs Delay

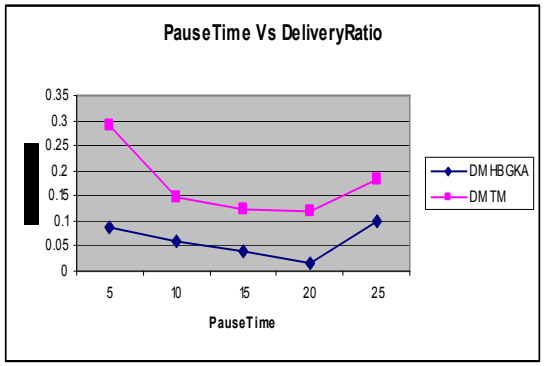

Figure 13: Pause Time Vs Delivery Ratio

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

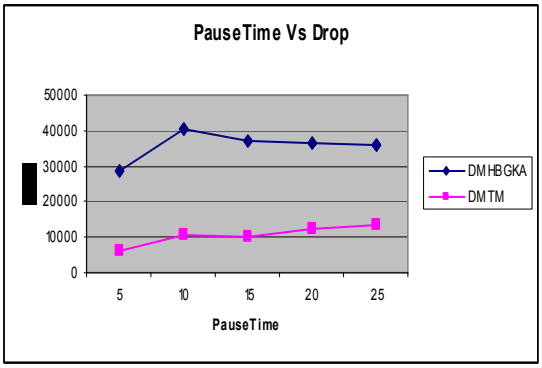

Figure 14: Pause Time Vs Drop

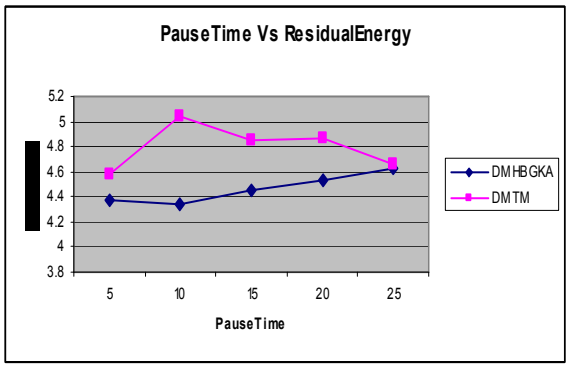

Figure 15: Pause Time Vs Residual Energy

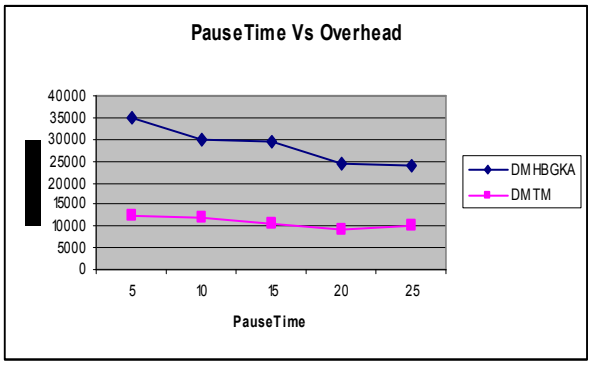

Figure 16: Pause Time Vs Overhead

Figure 12 shows the authentication delay measured for DMHBGKA and DMTM when the pause time is varied. However, the average delay of DMTM is 5% lesser when compared to DMHBGKA, since it involves polynomial based group key generation process, which is less complex when compared to ECDH of DMHBGKA.

Figure 13 shows the packet delivery ratio measured for DMHBGKA and DMTM when the pause time is varied. Since DMTM provides both intra and inter GKM, the average delivery ratio of DMTM is 65% of higher than DMHBGKA.

Figure 14 shows the packet drop measured for DMHBGKA and DMTM when the pause time is varied. Since DMTM provides both intra and inter GKM, the average packet drop of DMTM is 71% lesser than DMHBGKA.

Figure 15 shows the residual energy measured for DMHBGKA and DMTM when the pause time is varied. Since DMTM selects the group heads based on their energy level, the average residual energy of DMTM is 7% high when compared to DMHBGKA.

Figure 16 shows the overhead measured for DMHBGKA and DMTM when the pause time is varied. However, the DMTM has 62% reduced overhead when compared to DMHBGKA.

5. CONCLUSION

In this paper, we have proposed a Dynamic Multicast Height Balanced Group Key Agreement (DMHBGKA) technique to overcome the cost issue seen in MANET whenever any node enters or leaves the network. This is achieved by considering only the subtree which includes the new node or deleted node for group key creation. Initially, we have considered the case in which new node/nodes enter into the network. Whenever a new node joins a network multicast tree, the tree structure is examined for imbalance. If imbalance is identified, then the nodes in the subtree containing the new node is rotated either left or right based on type of imbalance. Next, when any node leaves the network multicast tree, the imbalance is identified based on balance factor. On detection of imbalance, the departed node information is collected and the remaining nodes in the corresponding subtree is rotated accordingly. In this way, balance in the network is maintained in a cost effective manner and without much overhead. The proposed technique can be applied on applications involving group chat and conferences etc,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

where the communications need security and less cost. Though this work aims to provide secure communication, it does not protect from insider attacks, which can be considered as a future work.

REFERENCES

[1]. G Nagaraja, and Pradeep Reddy CH, "A SURVEY ON GROUP KEY MANAGEMENT FRAMEWORKS FOR SECURE GROUP COMMUNICATION IN MOBILE AD HOC NETWORKS", *International Journal Of Pharmacy & Technology*, 2016,ISSN: 0975-766X, CODEN: *IJPTFI.*

[2]. G.Narayana, M.Akkalakshmi and A.Damodaram, "Energy Efficient Polynomial Based Group Key Management Protocol for Secure Group Communications in MANET", *International Journal of Applied Engineering Research* ISSN 0973-4562 Volume 11, Number 9, 2016,pp 6701-6705.

[3]. Y ongdae Kim, Adrian Perrig, and Gene Tsudik "T ree-based Group Key Agreement", ACM,2004.

[4]. Yanji Piao, JongUk Kim, Usman Tariq, Manpyo Hong "Polynomial-based key management for secure intra-group and inter-group communication", *Elsevier* ,2012.

[5]. B. Gopalakrishnan, T. V. P. Sundararajan and Dr. A. Shanmugam, "AGPM: An Authenticated Secure Group Communication Protocol for MANETs", *International Journal of Recent Trends in Engineering*, Vol 1, No. 1, May 2009.

[6]. V. Palanisamy and P. Annadurai, "Secure Group Communication using Multicast Key Distribution Scheme in Ad hoc Network (SGCMKDS)", *International Journal of Computer Applications* (0975 - 8887), Volume 1 – No. 25,2010.

[7]. B. Gopalakrishnan, and Dr. A. Shanmugam, "EETSS: Energy Efficient Transitive Signature Scheme for Secure Group Communication in MANETs", *International Journal of Engineering and Technology (IJET),*2013.

[8]. N. Vimala, B. Jayaram, and Dr. R. Balasubramanian, "Efficient Group Key Management Protocol for Region Based MANETs", *IACSIT International Journal of Engineering and Technology*, Vol.3, No.1, February 2011, ISSN: 1793-8236

[9]. Hua-Yi Lin and Tzu-Chiang Chiang, "Efficient Key Agreements in Dynamic Multicast Height Balanced Tree for Secure Multicast Communications in Ad Hoc Networks", *Hindawi Publishing Corporation, EURASIP Journal on Wireless Communications and Networking*, Volume 2011, Article ID 382701,15pages, doi:10.1155/2011/382701

[10]. G. Narayana and A. Damodaram, "Energy Efficient Polynomial Based Group Key Management Protocol for Secure Group Communications in MANET", *International Journal of Applied Engineering Research* ISSN 0973-4562 Volume 11, Number 9,2016, pp 6701-6705.

[11]. G.Narayana, M.Akkalakshmi and A.Damodaram,"Intra and Inter Group Key Authentication for Secure Group Communication in MANET", *4th INTERNATIONAL CONFERENCE on INNOVATIONS IN COMPUTER SCIENCE & ENGINEERING*, Springer,2016.